CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

1. (original) A method comprising:

enabling at least one client to access restricted information from an origin web-server through a semi-trusted web-server including the steps of:

authenticating said at least one client;

creating a client credential having client-specific environment information for each said at least one client;

presenting the client credential to the semi-trusted web-server;

correlating said at least one client with the client credential; and

providing said access to said at least one client.

2. (original) A method as recited in claim 1, further comprising serving the restricted information to said at least one client through the semi-trusted web-server.

3. (original) A method as in claim 1, wherein the step of creating comprises storing the client-specific environment information and the client credential in a cookie in said at least one client's browser.

4. (original) A method as in claim 1, wherein the step of presenting comprises:

sending the client credential to the semi-trusted web-server; and

using HTTP redirection to refer said at least one client to the semi-trusted web-server. (original)

5. (original) A method as in claim 1, wherein the step of presenting comprises:

sending said at least one client credential to a directory accessible to the semi-trusted web-server; and

the origin web-server using HTTP redirection to send said at least one client to the semi-trusted web-server.

6. (original) A method as in claim 1, wherein the step of creating comprises:

collecting the client-specific environment information; and

storing the client-specific environment information in the client credential.

7. (original) A method as in claim 6, wherein the client-specific environment information includes:

a hash of the HTTP-Request header of said at least one client request;

a hash of the IP address of the machine used by said at least one client;

a process identity of said at least one client browser;

a hash of a user identity used by said at least one client program; and/or

any combination of these.

8. (original) A method as in claim 1, wherein the step of creating comprises:

placing a first client-side program at said at least one client;

collecting a first set of the client-specific environment information using the first client-side program;

sending the first set of the client-specific environment information to the origin web-server; and

storing the first set of the client-specific environment information in the client credential.

9. (original) A method as in claim 8, wherein the step of correlating includes:

the semi-trusted web-server placing a second client-side program at said at least one client;

collecting a second set of the client-specific environment information with the second client-side program;

sending the second set of the client-specific environment information to the semi-trusted web-server; and

correlating the second set of the client-specific environment information to the client credential.

10. (original) A method as in claim 9, wherein the first and/or the second client-specific environment information includes: a hash of the HTTP-Request header of said at least one client request; a hash of the IP address of the machine used by said at least one client; a process identity

of said at least one client browser; a hash of a user identity used by said at least one client program; and/or any combination of these.

11. (original) A method as in claim 1, further comprising the semi-trusted web-server accessing an encrypted version of the restricted information, and wherein the step of creating the client credential includes adding a decryption key to the client credential.

12. (original) A method as in claim 11 wherein the decryption key is a partial key, and the step of providing includes the semi-trusted web-server supplying information to said at least one client enabling conversion of the partial key to a full key.

13. (original) A method as in claim 1 wherein the step of authenticating includes employing a user-password scheme.

14. (original) A method as in claim 1, wherein the step of authenticating includes deploying at least one certificate.

15. (original) A method as in claim 6, wherein the step of collecting the client-specific environment information is performed by the origin web-server, and

the origin web-server storing the client-specific environment information in the client credential.

16. (original) A method as in claim 8, wherein the steps of placing and the step of storing is performed by the origin web-server.

17. (original) A method as recited in claim 1, wherein the semi-trusted web-server is a proxy web-server.

18. (original) A method as recited in claim 1, wherein the step of creating a credential for said at least one client at an origin web-server;

19. (original) A method as recited in claim 1, wherein the step of correlating said at least one client and the client credential is performed by the semi-trusted web-server.

20. (original) A method as recited in claim 1, wherein the step of authenticating said at least one client is performed at the origin web-server.

21. (currently amended) An apparatus for enabling at least one client to access restricted information from an origin web-server through a semi-trusted web-server, said apparatus comprising:

an authenticator to validate said at least one client;

a credential creator to create a client credential having client-specific environment information for each said at least one client; and

a correlator for matching said at least one client to the client credential, and for working in combination with said authenticator and said credential creator to enable said at least one client to safely access restricted information from the origin web-server through the semi-trusted web-server.

22. (original) The apparatus as in claim 21, wherein the credential creator stores the client-specific environment information in a cookie set in said at least one client's browser.

23. (original) An apparatus as in claim 21, wherein the credential creator presents the credential to the semi-trusted web-server.

24. (original) The apparatus as in claim 21, wherein the credential creator stores a client-side program in said at least one client's browser.

25. (original) The apparatus as in claim 21, wherein the correlator stores a second client-side program in the client's browser.

26. (original) The apparatus as in claim 21, wherein the semi-trusted web-server has access only to an encrypted version of the restricted information, and the credential creator adds a decryption key to the client credential.

27. (original) The apparatus as in claim 26, wherein the decryption key is a partial key and the semi-trusted web-server includes an information supplier to supply said at least one client with information to enable conversion of the partial key to a full key.

28. (original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for enabling at least one client to access restricted information from an origin web-server through a semi-trusted web-server, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

29: An article of manufacture as recited in claim 28, the computer readable program code means in said article of manufacture further comprising computer readable program code means for causing a computer to effect the steps of claim 12.

30. (original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for enabling at least one client to access restricted information from an origin web-server through a semi-trusted web-server, said method steps comprising the steps of claim 1.

31. (original) An apparatus comprising:

means for enabling at least one client to access restricted information from an origin web-server through a semi-trusted web-server including:

means for authenticating said at least one client;

means for creating a client credential having client-specific environment information for each said at least one client;

means for presenting the client credential to the semi-trusted web-server;

means for correlating said at least one client with the client credential; and

means for providing said access to said at least one client.

32. (original) An apparatus as recited in claim 31, further comprising means for serving the restricted information to said at least one client through the semi-trusted web-server.

33. (original) An apparatus as in claim 31, further comprising means for storing the client-specific environment information and the client credential in a cookie in said at least one client's browser.

34. (original) An apparatus as in claim 31, further comprising means for:

sending the client credential to the semi-trusted web-server; and

using HTTP redirection to refer said at least one client to the semi-trusted web-server. (original)

35. (original) An apparatus as in claim 31, wherein the origin web-server uses HTTP redirection to send said at least one client to the semi-trusted web-server, and further comprising means for sending said at least one client credential to a directory accessible to the semi-trusted web-server.

36. (original) An apparatus as in claim 31, further comprising means for:

collecting the client-specific environment information; and

storing the client-specific environment information in the client credential.

37. (original) An apparatus as in claim 36, wherein the client-specific environment information includes:

a hash of the HTTP-Request header of said at least one client request;

a hash of the IP address of the machine used by said at least one client;

a process identity of said at least one client browser;

a hash of a user identity used by said at least one client program; and/or

any combination of these.

38. (original) An apparatus as in claim 31, further comprising means for:

placing a first client-side program at said at least one client;

collecting a first set of the client-specific environment information using the first client-side program;

sending the first set of the client-specific environment information to the origin web-server; and

storing the first set of the client-specific environment information in the client credential.

39. (original) An apparatus as in claim 38, further comprising means for:

the semi-trusted web-server to place a second client-side program at said at least one client;

collecting a second set of the client-specific environment information with the second client-side program;

sending the second set of the client-specific environment information to the semi-trusted web-server; and

correlating the second set of the client-specific environment information to the client credential.

40. (original) An apparatus as in claim 39, wherein the first and/or the second client-specific environment information includes:

a hash of the HTTP-Request header of said at least one client request;

a hash of the IP address of the machine used by said at least one client;

a process identity of said at least one client browser;

a hash of a user identity used by said at least one client program;

and/or any combination of these.

41. (original) An apparatus as in claim 31, further comprising means for the semi-trusted web-server to access an encrypted version of the restricted information, and means for adding a decryption key to the client credential during creation.

42. (original) An apparatus as in claim 41, wherein the decryption key is a partial key comprising means for the semi-trusted web-server to supply information to said at least one client enabling conversion of the partial key to a full key.

43. (original) An apparatus as in claim 31, further comprising of a means for authenticating by employing a user-password scheme.

44. (original) An apparatus as in claim 31, further comprising of a means for authenticating by deploying at least one certificate.

45. (original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing enablement of at least one client to access restricted information from an origin web-server through a semi-trusted web-server, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the apparatus of claim 31.

46. (original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing enablement of at least one client to access restricted information from an origin web-server through a semi-trusted web-server, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the apparatus of claim 21.